CALEA

11-14 minutes

COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT (CALEA)

The Perils of Wiretapping the Internet

EFF and a coalition of public interest, industry, and academic groups filed suit in 2005 challenging the Federal Communications Commission's (FCC) unjustified expansion of the Communications Assistance for Law Enforcement Act (CALEA). By forcing broadband Internet and interconnected voice over Internet Protocol (VoIP) services to become wiretap-friendly, the FCC ignored CALEA's plain language and threatened privacy, security, and innovation.

Congress passed the Communications Assistance for Law Enforcement Act (CALEA) in 1994 to make it easier for law enforcement to wiretap digital telephone networks. CALEA forced telephone companies to redesign their network architectures to make wiretapping easier. It expressly did not regulate data traveling over the Internet.

But now federal law enforcement agencies want to change that. On March 10, 2004, the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), and the Drug Enforcement Administration (DEA) filed a joint petition with the FCC. The petition requested that CALEA's reach be expanded to cover communications that travel over the Internet. Thus, Broadband providers would be required to rebuild their networks to make it easier for law enforcement to tap Internet "phone calls" that use VOIP applications such as Vonage, as well as online "conversations" using various kinds of instant messaging (IM) programs like AOL Instant Messenger (AIM).

EFF objected to a number of the requests in the joint petition, in conjunction with numerous other organizations.

On August 9, 2004, the Federal Communications Commission (FCC) released its Notice of Proposed Rulemaking (NPRM) in response to the Law Enforcement joint petition. Applying dubious legal reasoning, it greatly expands the reach of CALEA by redefining what constitutes a "substantial replacement" of the telephone service, tentatively concluding that broadband Internet access providers and managed VoIP systems substantially replace local exchanges, and therefore are subject to the requirements of CALEA. (See CALEA Summary.)

On August 5, 2005, the FCC announced a Final Rule, expanding CALEA to Internet broadband providers and certain Voice-over-IP (VoIP) providers.

The FCC ruling has been challenged in court by EFF and others and may end up before the

Supreme Court. After the DC Circuit Court of Appeals' ruling, the coalition of challengers filed for en banc review.

- DC Circuit Court opinion [PDF, 414k]
- Petition for Rehearing En Banc [PDF, 529k]

Meanwhile, the DOJ—apparently tired of our lawsuits and hoping to avoid such suits in the future—has now proposed draft legislation to codify and expand the FCC ruling.

- DeepLink: Administration Laughs at CALEA, Proposes to Eviscerate Law's Compromise *July 25, 2006*
- Draft of legislation [PDF, 759k]
- Section-by-section Analysis [PDF, 769k]

Wiretapping Is Already Easy Enough

Law enforcement agencies convinced the FCC that CALEA needed to be expanded in order to maintain the status quo. Because wiretapping has gotten so much more complex in the Internet age, they argued, it's just too hard for them to intercept all the communications that they need. Without structural changes to the Internet, they won't be able to conduct the same quality of investigations that they did ten years ago.

It is crucial to remember that the issue here is not whether law enforcement can tap new technologies like VoIP, but whether they can tap it easily. Existing laws already permit law enforcement to place Internet users under surveillance, regardless of what programs or protocols they are using to communicate. Industry already cooperates with law enforcement to give it all the information requested, and this will continue to happen with or without a new FCC rule interpreting CALEA.

Ironically, most kinds of surveillance have gotten much easier in the digital age. Agents can tap mobile phones, gain access to reams of electronic communications such as email, conduct DNA identification tests, and track people's locations using cell phone signals. Surely the greater ease of surveillance in these arenas and others more than makes up for the negligible difficulty of capturing a few VoIP calls and IM conversations. We would be maintaining the status quo without expanding CALEA.

Just Because It Can Be Tapped Doesn't Mean It Should

The FBI used the "tappability principle" to justify the demands in its petition. This principle holds that if something is legally searchable sometimes, it should be physically searchable all the time. But there is a vast difference between a computer network switch created precisely to be tappable and one that can be tapped with the right tools under the right circumstances. If we applied the FBI's logic to the phone system, it would state that every individual phone should be designed with built-in bugs. Consumers would simply have to trust law enforcement or the phone companies not to activate those bugs without just cause.

The Cost of CALEA Will Be Passed on to Consumers

The NPRM's proposed expansion of CALEA would also punish broadband providers and consumers, concluding that carriers should forced to spend millions of dollars on CALEA compliance. The FCC explores a mechanism by which these costs will pass to their customers, including a Commission mandated flat monthly charge. Quite literally, then,

consumers would be subsidizing the surveillance state.

Furthermore, this proposal completely restructures market incentives in the technology industry. Privacy-friendly technologies, which protect the personal information of consumers, would be pushed out of the marketplace. Instead, companies would be forced to design and manufacture surveillance-friendly technologies. The needs of government, not consumers, would guide the marketplace.

Innovation Will Suffer

When special interests like law enforcement commandeer the marketplace, innovation suffers. The NPRM suggests that all devices that provide broadband connectivity will have to be CALEA-compliant, which would severely limit the scope of high-tech research and development. Today's VoIP systems — revolutionary software tools that allow people to make phone calls over the Internet — would likely never have been developed in an environment where all products had to go through a CALEA-compliance test before making it to market. While the NPRM does not extend CALEA to providers of peer-to-peer VoIP, email and Instant Messaging, it seeks comment on whether other laws might give the FCC power over a wider array of technologies.

If the FBI gets its way, the NPRM's tentative regulations will only be the tip of the iceberg. Soon, software companies, under threat of an expansive definition of CALEA's requirements, will face economic incentives to create email and IM programs that are surveillance-ready. Many computer game consoles that people can use to play over the Internet, such as the Xbox, allow gamers to chat with each other while they play. If any communication program running on the Internet has to be CALEA-compliant before being bought and sold, what would stop law enforcement from pushing for a tappable Xbox?

CALEA means that innovators will always be forced to think inside the box of surveillance. Their designs and ideas will be limited by a government mandate that requires them to build technology for the purpose of spying rather than playing games, talking to colleagues, or collaboratively making art over the Internet. This will stifle creativity and result in a non-competitive technology market. The only creativity will exist off-shore, where developers outside the U.S. will develop technologies to circumvent U.S. law enforcement capability.

The Internet Is Not Like the Phone System

The NPRM suggests that rules applied to the phone system should also be applied to the Internet. But crucial differences between the two systems mean that what is healthy for one in terms of marketplace incentives and technological development is unhealthy for the other. What makes the Internet powerful are its edges: computers and other innovative technologies are located at the ends of the network wires. The phone system works the opposite way. Telephones are dumb, inflexible machines. Whereas the usefulness of the phone system comes from the telecommunications network itself, the Internet's usefulness comes from its endpoints.

In addition, the phone network is a closed, insulated system, while the Internet is open and ever-changing. End users cannot change the nature of the phone network on a whim. But on the Internet, people can deploy new services and new devices at will — they can invent new protocols for sending data, or connect a new kind of widget to the network. This is integral to making the Internet a vital source of technological and scientific innovation.

EFF believes that federal agencies should not force the broadband Internet access or voice over IP industries, and by extension, their consumers, to bear the considerable costs of purchasing and implementing surveillance-ready network technologies simply because it suits the government's needs.

CALEA Could Make the Internet Less Secure

While law enforcement's efforts to hijack the tech market are disturbing, EFF is also concerned that making the Internet CALEA-compliant might backfire: many of the technologies currently used to create wiretap-friendly computer networks make the people on those networks more pregnable to attackers who want to steal their data or personal information.

When broadband service providers are forced to make their networks or applications tappable, this introduces more points of vulnerability into the system. Users have to place blind trust in companies and services they may not realize they are signing up for.

The FCC's proposes to allow third parties to manage government surveillance requests: a private company would analyze all the data from a telecommunications carrier, extract information relevant to the court order, and send it to law enforcement.

Currently, several large corporations are already offering CALEA services that might result in a loss of privacy for consumers. For example, VeriSign offers a legal intercept service to ISPs, which requires the providers to pipe all their data to VeriSign. Then the company's employees analyze the data, extract information relevant to the court order, and send it to law enforcement. This transaction leaves personal data potentially vulnerable when it travels from the service provider's network to VeriSign's. It also places the personal data of innocent people in the hands of a third party without customer consent. If CALEA is applied to the Internet, it is likely that many more services like VeriSign's will spring up, introducing still more uncertainty into the system.

Services like these support and expand what the ACLU has called the Surveillance-Industrial Complex. Since compliance with surveillance requests is a significant cost for carriers, telecommunications companies have acted as a check on government power, lobbying against excessive proposals. Now, private entities that profit from surveillance will have an incentive to lobby for more government surveillance powers.

Ultimately, all of these problems can be traced back to a single root cause: CALEA was drafted specifically to regulate phone networks, which are designed to be closed systems. The Internet is an open, global system that handles countless forms of data-transfer and accommodates an ever-changing array of smart edge-devices. If CALEA is misapplied to the Internet, the results will be disastrous. The privacy of innocent people is likely to be violated, innovation will certainly be stifled, and the current and future functionality of the Internet will be crippled.